(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－34164
（P2001－34164A）
(43)公開日　平成13年２月９日(2001.2.9)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ａ	５Ｂ０１７
	６４０		６４０Ｂ	５Ｊ１０４
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｚ	
9/10			６２１Ａ	

審査請求　有　　請求項の数７　ＯＬ　（全 19 頁）

(21)出願番号　特願平11－209891

(22)出願日　平成11年７月23日(1999.7.23)

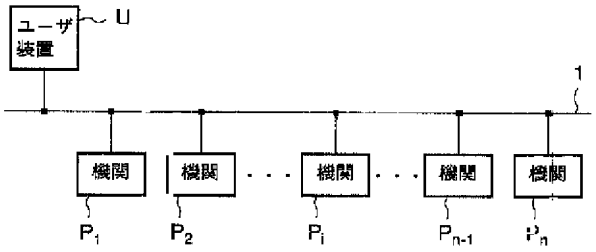
特許法第30条第１項適用申請有り　1999年１月26日～１月29日　電子情報通信学会情報セキュリティ研究専門委員会主催の「1999年暗号と情報セキュリティシンポジウム」において文書をもって発表

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　櫻井　幸一
福岡県福岡市東区箱崎６丁目10番１号　九州大学内
(72)発明者　宮崎　真悟
東京都府中市東芝町１番地　株式会社東芝府中工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　秘密分散システム及び記憶媒体

(57)【要約】
【課題】　本発明は、分配者の無い環境で秘密鍵を算出せずに、ｎ個の機関のうち、任意ｔ個の機関による分散復号や署名の実現を図る。
【解決手段】　ｎ個の各機関Ｐ１～Ｐｎが、（ｎ，ｎ）型の１個の部分情報ｄｉ（０≦ｉ≦ｎ）を保持し、部分情報ｄｉを（ｔ，ｎ）型のｔ（ｒ＋１）個の部分乱数Ｓｊとし、ｒ＋１個の部分乱数Ｓｊを各機関Ｐｉの識別番号ｚのｔ進表示（t^j桁目の値ｋ、０≦ｋ≦ｔ－１、０≦ｊ≦ｒ）に基づいて、各々機関Ｐ１～Ｐｎに分散し、互いに分散された部分乱数をｔ進表示の桁t^j毎にまとめてｒ＋１個の部分情報ｄｊ,ｋを得る。次に、ユーザ装置Ｕがｔ個の機関Ｔｚを選択して暗号化データＣを送信し、ｔ個の機関Ｔｚが暗号化データＣを部分情報ｄｊ,ｋに基づき演算処理して得た部分出力Ｘｚをそれぞれユーザ装置Ｕに返信し、ユーザ装置Ｕがｔ個の部分出力Ｘｚを合成して復号結果を得る秘密分散システム及び記憶媒体。



【特許請求の範囲】
【請求項１】　素因数分解問題に基づく暗号系に用いられ、ｎ個の機関に秘密鍵の部分最終情報が分散され、且つ、いずれの機関も自己の部分最終情報だけでは前記秘密鍵を算出不可能な環境にあるとき、前記ｎ個の機関のうち、任意のｔ個の機関により、前記秘密鍵を算出せずに復号結果及び署名結果を生成可能な（ｔ，ｎ）型の秘密分散システム。
【請求項２】　公開鍵及び秘密鍵ｄを用いるＲＳＡ暗号系に適用され、互いにネットワークを介して接続されたｎ個の機関及びユーザ装置を備え、ｎ個の機関に前記秘密鍵ｄの部分最終情報が分散されたとき、その中の任意のｔ個の機関により、前記秘密鍵ｄを算出せずに復号結果又は署名結果を生成可能な（ｔ，ｎ）型の秘密分散システムであって、
前記ｎ個の各機関は、
前記公開鍵及び前記秘密鍵ｄを生成する手段と、
この秘密鍵ｄに基づいて生成された（ｎ，ｎ）型の１個の部分情報ｄｉ（０≦ｉ≦ｎ）を保持する手段と、
ｔを底としたｎの対数$\log_t$ｎ以上の最小の整数をｒとしたとき、前記部分情報ｄｉを（ｔ，ｎ）型のｔ（ｒ＋１）個の部分乱数とし、そのうちのｒ＋１個の部分乱数を前記各機関の識別番号のｔ進表示（t^j桁目の値ｋ、０≦ｋ≦ｔ－１、０≦ｊ≦ｒ）に基づいて、それぞれ各機関に分散する手段と、
前記各機関から分散されたｎ（ｒ＋１）個の部分乱数をｔ進表示の桁t^j毎にまとめてｒ＋１個の部分最終情報ｄｊ,ｋを得る手段と、
前記ユーザ装置から受けた処理対象データを前記部分最終情報ｄｊ,ｋに基づいて演算処理し、得られた部分出力を前記ユーザ装置に返信する手段とを有し、
前記ユーザ装置は、
前記ｔ個の機関を選択し、この選択したｔ個の各機関に処理対象データを送信する手段と、
前記ｔ個の各機関から受信した部分出力を合成して前記復号結果又は署名結果を得る手段とを備えたことを特徴とする秘密分散システム。
【請求項３】　第１の公開鍵（ｅ，Ｎ）及び秘密鍵ｄと、第２の公開鍵（L^2，Ｎ）とを用いるＲＳＡ暗号系（ｅとL^2とは最大公約数が１であり、法Ｎは共通）に適用され、互いにネットワークを介して接続されたｎ個の機関及びユーザ装置を備え、ｎ個の機関に前記秘密鍵ｄの部分情報ｓｊが分散されたとき、その中の任意のｔ個の機関により、前記秘密鍵ｄを算出せずに復号結果を生成可能な（ｔ，ｎ）型の秘密分散システムであって、
前記ｎ個の各機関は、
前記ユーザ装置から受けた復号対象データＣ２（＝M^e　（ｍｏｄ　Ｎ））を演算処理して得られた部分出力Ｚｊを前記ユーザ装置に返信する手段とを有し、
前記ユーザ装置は、
前記ｎ個の機関のうちのｔ個の機関を選択し、この選択したｔ個の各機関に前記復号対象データＣ２を送信する手段と、
前記ｔ個の各機関から受信した部分出力Ｚｊを合成して前記復号結果Ｃ１（＝$M^{L\hat{}2}$　（ｍｏｄ　Ｎ）、^はべき乗を示す記号）を得る手段と、
前記復号結果Ｃ１、前記処理対象データＣ２及び下記式に基づいて、演算処理を実行し、最終復号結果Ｍを求める手段とを備えたことを特徴とする秘密分散システム。
$a1=(L^2)^{-1}$　（ｍｏｄ　ｅ）
$a2=(a1L^2-1)/e$
$M=C_1^{a1}(C_2^{a2})^{-1}$　（ｍｏｄ　Ｎ）
【請求項４】　請求項３に記載の秘密分散システムにおいて、
前記復号対象データＣ２に代えて、署名対象データＳ２（＝Ｍ）を用い、
前記復号結果Ｃ１に代えて、署名結果Ｓ１（＝$M^{d\ L\hat{}2}$（ｍｏｄ　Ｎ）、^はべき乗を示す記号）を用い、
前記最終復号結果Ｍを求める手段に代えて、
前記署名結果Ｓ１（＝$(M^d)^e$）、前記署名対象データＳ２（＝$(M^d)^{L\hat{}2}$）及び下記式に基づいて、演算処理を実行し、最終署名結果M^dを求める手段とを備えたことを特徴とする秘密分散システム。
$a1=(L^2)^{-1}$　（ｍｏｄ　ｅ）
$a2=(a1L^2-1)/e$
$M^d=S_1^{a1}(S_2^{a2})^{-1}$　（ｍｏｄ　Ｎ）
【請求項５】　公開鍵及び秘密鍵ｄを用いるＲＳＡ暗号系に適用され、互いにネットワークを介して接続されたｎ個の機関及びユーザ装置を備え、ｎ個の機関に前記秘密鍵ｄの部分最終情報が分散されたとき、その中の任意のｔ個の機関により、前記秘密鍵ｄを算出せずに復号結果又は署名結果を生成可能な（ｔ，ｎ）型の秘密分散システムに使用されるコンピュータ読み取り可能な記憶媒体であって、
前記ｎ個の各機関内のコンピュータに、
前記公開鍵及び前記秘密鍵ｄを生成する手段と、
この秘密鍵ｄに基づいて生成された（ｎ，ｎ）型の１個の部分情報ｄｉ（０≦ｉ≦ｎ）を保持する手段と、
ｔを底としたｎの対数$\log_t$ｎ以上の最小の整数をｒとしたとき、前記部分情報ｄｉを（ｔ，ｎ）型のｔ（ｒ＋１）個の部分乱数とし、そのうちのｒ＋１個の部分乱数を前記各機関の識別番号のｔ進表示（t^j桁目の値ｋ、０≦ｋ≦ｔ－１、０≦ｊ≦ｒ）に基づいて、それぞれ各機関に分散する手段と、
前記各機関から分散されたｎ（ｒ＋１）個の部分乱数をｔ進表示の桁t^j毎にまとめてｒ＋１個の部分最終情報ｄｊ,ｋを得る手段、
前記ユーザ装置から受けた処理対象データを前記部分最終情報ｄｊ,ｋに基づいて演算処理し、得られた部分出力を前記ユーザ装置に返信する手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項６】　第１の公開鍵（ｅ，Ｎ）及び秘密鍵ｄと、第２の公開鍵（L^2，Ｎ）とを用いるＲＳＡ暗号系（ｅとL^2とは最大公約数が１であり、法Ｎは共通）に適用され、互いにネットワークを介して接続されたｎ個の機関及びユーザ装置を備え、ｎ個の機関に前記秘密鍵ｄの部分情報ｓｊが分散されたとき、その中の任意のｔ個の機関により、前記秘密鍵ｄを算出せずに復号結果を生成可能な（ｔ，ｎ）型の秘密分散システムに使用される記憶媒体であって、

前記ｎ個の各機関内のコンピュータに、

前記ユーザ装置から受けた復号対象データＣ２（$=M^e$　（ｍｏｄ　Ｎ））を演算処理して得られた部分出力Ｚｊを前記ユーザ装置に返信する手段、を実現させるためのプログラムを記憶し、

前記ユーザ装置内のコンピュータに、

前記ｎ個の機関のうちのｔ個の機関を選択し、この選択したｔ個の各機関に前記復号対象データＣ２を送信する手段、

前記ｔ個の各機関から受信した部分出力Ｚｊを合成して前記復号結果Ｃ１（$=M^{L\hat{}2}$　（ｍｏｄ　Ｎ）、^はべき乗を示す記号）を得る手段、

前記復号結果Ｃ１、前記処理対象データＣ２及び下記式に基づいて、演算処理を実行し、最終復号結果Ｍを求める手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

$a1=(L^2)^{-1}$　（ｍｏｄ　ｅ）

$a2=(a1L^2-1)/e$

$M=C_1^{a1}(C_2^{a2})^{-1}$　（ｍｏｄ　Ｎ）

【請求項７】　請求項６に記載の記憶媒体において、

前記復号対象データＣ２に代えて、署名対象データＳ２（＝Ｍ）を用い、

前記復号結果Ｃ１に代えて、署名結果Ｓ１（$=M^{d\ L\hat{}2}$（ｍｏｄ　Ｎ）、^はべき乗を示す記号）を用い、

前記最終復号結果Ｍを求める手段に代えて、

前記署名結果Ｓ１（$=(M^d)^e$）、前記署名対象データＳ２（$=(M^d)^{L\hat{}2}$）及び下記式に基づいて、演算処理を実行し、最終署名結果M^dを求める手段とを実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

$a1=(L^2)^{-1}$　（ｍｏｄ　ｅ）

$a2=(a1L^2-1)/e$

$M^d=S_1^{a1}(S_2^{a2})^{-1}$　（ｍｏｄ　Ｎ）

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、素因数分解問題に基づく暗号系の秘密分散システム及び記憶媒体に係り、特に、ｎ個の機関に秘密鍵を秘密分散し、その中の任意のｔ個の機関により、秘密鍵を算出せずに分散復号及び署名を実現し得る秘密分散システム及び記憶媒体に関する。

【０００２】

【従来の技術】従来、素因数分解問題に基づく暗号系として、例えばＲＳＡ暗号系を用いた秘密分散の分野では、しきい値法と呼ばれる秘密分散方式がある。ここで、しきい値法は、秘密情報をｎ個の部分情報に分散したとき、ｎ個中のｔ個の部分情報により秘密情報を完全に復元するが、ｔ－１個の部分情報では秘密情報を全く復元できないという、しきい値ｔを境にした秘密情報の復元特性をもっている（なお、１＜ｔ＜ｎ）。

【０００３】この種の秘密分散方式としては、ＲＳＡ暗号系に、しきい値法の概念を導入し、秘密鍵を（ｔ，ｎ）型で秘密分散させる（ｔ，ｎ）型の秘密分散方式が知られている（Y. Frankel, P. Gemmell, P. D. MacKenzie and M. Yung, Optimal-resilience proactive public-key cryptosystems, 38th Annual Symposium on Foundations of Computer Science, pp. 384-393, 1997.（以下、文献［ＦＧＭＹ９７］という）、及びT. Okamoto, Threshold key-recovery systems for RSA, Security Protocols, LNCS 1361, pp. 191-200, 1997.（以下、文献［Ｏｋａ９７］という））。

【０００４】中でも、文献［ＦＧＭＹ９７］は、ディーラー（分配者）の存在する環境において、秘密鍵ｄを算出せずに、任意ｔ個の機関で復号や署名の可能な方式を示している。すなわち、合成数Ｎの異なる素因数を知るディーラーが、素因数を知らなくても任意のｔ個の部分情報で復号や署名の可能な秘密鍵ｄを作成可能な方式である。

【０００５】一方、ディーラーの存在しない環境において、しきい値法ではなく、全ての機関で鍵生成を行う（ｎ，ｎ）型の秘密分散方式が知られている（D. Boneh and M. Franklin, Efficient generation of shared RSA keys, Advances in Cryptology-CRYPTO 97, LNCS 1294, pp. 425-439, 1997.（以下、文献［ＢＦ９７］という））。

【０００６】文献［ＢＦ９７］の方式では、鍵生成を実行すると、秘密鍵ｄに対して（ｎ，ｎ）型の秘密分散が同時に行われる。また、保持する部分情報を用いた全ての機関からの部分出力を合成することにより、秘密鍵ｄを算出せずに暗号文を復号可能となっている。

【０００７】詳しくは、文献［ＢＦ９７］では、以下にアルゴリズムを示すように、（２，２）型の秘密分散から（２，ｎ）型の秘密分散（$n \geq 3$を効率的に構築する方式が述べられている。

【０００８】なお、説明の簡単のため、秘密鍵ｄを知るユーザがいて、このユーザが秘密鍵ｄを（２，ｎ）型で秘密分散すると仮定する。また、機関Ｐの総数ｎに対し、部分情報の組合せを示す秘密分散多項式の個数は、

ｒ＋１であるとし、ｒ＝「ｌｏｇ　ｎ」であるとする（本明細書中、「」は、その括弧内の値以上の最小の整数を示す）。

【０００９】まず、ユーザは、（２，２）型の秘密分散をｒ＋１回実行するため、ｒ＋１個の独立多項式ｄ＝$d_{0,0}+d_{0,1}=d_{1,0}+d_{1,1}=\cdots=d_{r,0}+d_{r,1}$を個別に作成する。

【００１０】次に、総数ｎの機関における個々の機関の識別番号をｚとし（ｚ　［０，ｎ］）、識別番号ｚの２進表示を$z(2)=\beta_r\ \beta_{r-1}\cdots\ \beta_0$とする。ユーザは、０番目～ｎ番目の全ての機関$P_0$～$P_n$を対象とし、順次、ｚ番目の機関$P_z$に、ｒ＋１個の部分情報：$\{d_{r,\beta r}, d_{r-1,\beta r-1}, \cdots, d_{0,\beta 0}\}$を送る。これにより、全ての機関$P_0$～$P_n$には、識別番号ｚの２進表示に対応する部分情報の集合が配送される。

【００１１】配送完了後、機関の番号を唯一に設定することで、任意の２個の機関Ｐｉ，Ｐｊ（ｉ≠ｊ）は、ｒ＋１個の（２，２）型の部分情報のうち、番号ｚ（２）で互いにビットβの異なる同一桁ｉの部分情報（$d_{i,0}$，$d_{i,1}$）から、秘密鍵ｄを復元可能となっている（$d_{i,0}+d_{i,1}=d$）。

【００１２】次に、上述した（２，２）型から（２，ｎ）型の秘密分散を構築する方式のように、秘密分散の型を拡張するための関連技術について述べる。この種の技術としては、（ｔ，１）型を用いた（ｔ，1^m）型の秘密分散方式がある（S. R. Blackburm, M. Burmester, Y. Desmedt and P. R. Wild, Efficient multiplicative sharing schemes, Advances in Cryptology-EUROCRYPT 96, pp. 107-118, 1996.（以下、文献［ＢＢＤＷ９６］という））。但し、文献［ＢＢＤＷ９６］の方式は、正の整数ｍに対し、次の（１）式を満たす１に関するものである。

【００１３】

【数１】

$$l \geq \binom{t}{2}(m-1) \qquad \cdots(1)$$

ここで、$b=\binom{t}{2}(m-1)$　とすると、

【００１４】

ｔ＝２　ｂ≧１　→　ｌ≧１

ｔ＝３　ｂ≧３　→　ｌ≧３

ｔ＝４　ｂ≧６　→　ｌ≧６

となり、ｔ≧４ではｔ＜ｌとなる。すなわち、ｔ≧４では、（ｔ，ｔ）型を用いた（ｔ，ｎ）型の秘密分散方式を構築不可能となっている。

【００１５】このため、以下では、同文献［ＢＢＤＷ９６］における（３，３）型を用いた（３，3^3）型の秘密分散方式を説明する。ｍ＝２，ｌ＝３，ｔ＝３とし、（２）式に示すように、ｂを算出する。

【００１６】

【数２】

$$b=\binom{t}{2}(m-1)=3 \qquad \cdots(2)$$

【００１７】まず、（３，３）型の秘密分散をｂ＋１＝４回実行し、（３）式に示すように、秘密鍵ｄに対する４つの独立多項式を構築する。

【００１８】

$d=d_{0,0}+d_{0,1}\vdash d_{0,2}$　（１回目）

$=d_{1,0}+d_{1,1}\vdash d_{1,2}$　（２回目）

$=d_{2,0}+d_{2,1}\vdash d_{2,2}$　（３回目）

$=d_{3,0}+d_{3,1}\vdash d_{3,2}$　（４回目）　…（３）

また、ｆ（ｘ）＝a_0+a_1X　（ｍｏｄ　３）とする。

【００１９】ここで、同文献［ＢＢＤＷ９６］では、最終的な機関（ここでは3^2個の機関）の集合をＰ´としたとき、ｆ（Ｘ）は（４）式のように記載される（pp.113の１行目、なお、式中の“ｄ”は、本明細書中では“ｍ”と表記した）。

【００２０】

【数３】

$$f(X)\to\sum_{i=0}^{d-1}a_iX^i\in P' \qquad \cdots(4)$$

【００２１】しかしながら、この（４）式は、次の（５）式の誤りと推測される。

【００２２】

【数４】

$$f(X)\cdot\sum_{i=0}^{d-1}a_iX^i(\mathrm{mod}\ \ell) \qquad \cdots(5)$$

【００２３】但し、a_0，a_1　F3であり、ｆ（∞）＝a_1とする。

【００２４】

ｆ１（ｘ）＝０　（ｍｏｄ　３）

ｆ２（ｘ）＝１　（ｍｏｄ　３）

ｆ３（ｘ）＝２　（ｍｏｄ　３）

ｆ４（ｘ）＝０＋Ｘ　（ｍｏｄ　３）

ｆ５（ｘ）＝１＋Ｘ　（ｍｏｄ　３）

ｆ６（ｘ）＝２＋Ｘ　（ｍｏｄ　３）

ｆ７（ｘ）＝０＋２Ｘ　（ｍｏｄ　３）

ｆ８（ｘ）＝１＋２Ｘ　（ｍｏｄ　３）

ｆ９（ｘ）＝２＋２Ｘ　（ｍｏｄ　３）

各機関ｆｊは（$d_{0,fj(\infty)}$，$d_{1,fj(0)}$，$d_{2,fj(1)}$，$d_{3,fj(2)}$）を持つ。具体的に各機関に保管される部分情報の集合は図１２に示す通りであり、機関の組合せと対象の部分情報は図１３に示す通りである。

【００２５】図１２に示すように、例えば機関ｆ１，ｆ４，ｆ８（２行目）で分散復号を行う際は、Ｘ＝∞に対応する部分情報を取り出す。それぞれ（$d_{0,0}$，$d_{0,1}$，$d_{0,2}$）による計算を行い、秘密鍵ｄに相当する出力を算出可能となっている。

【００２６】また、図１３中、ａ～１のいずれかのアルファベット符号の付された組合せは、各機関の同一の組合せにおいて、秘密鍵ｄに相当する出力の算出ルートが３種類あることを示している（なお、図１３中の“ｄ”は単なるアルファベット符号であり、秘密鍵ｄではない）。例えば符号ｂの付された機関の組合せ（ｆ１，ｆ２，ｆ３）では、Ｘ＝０，１，２の何れでも秘密鍵ｄを回復する３個の部分情報を揃えることが可能である。

【００２７】また一方、上述した文献［ＢＦ９７］における（ｎ，ｎ）型の秘密分散方式に対し、しきい値法の概念を導入した方式がある（Y. Frankel, P. D. MacKenzieand M. Yung, Robust efficient distributed RSA-key generation, Proceedings of the thirtieth annual ACM symposium on theory of computing, pp. 663-672, 1998.（以下、文献［ＦＭＹ９８］という））。

【００２８】文献［ＦＭＹ９８］の方式では、文献［ＢＦ９７］の（ｎ，ｎ）型の秘密分散に基づく（ｔ，ｎ）型の鍵生成・共有方式が示されている。具体的には、まず（ｎ，ｎ）型の鍵生成を行い、秘密鍵ｄに対する和の多項式を生成する。次に、各機関Ｐｉは、部分情報ｄｉのディーラーとなり、Sum-to-Poly（和から複数個へ）の変換を行う。このとき、各機関Ｐｉは、全ての機関Ｐｊからの部分情報ｄｊに対する共有情報を合成し、最終的に秘密鍵ｄに対する秘密分散を行って、秘密鍵ｄの（ｔ，ｎ）型の秘密共有を実現する。

【００２９】これにより、文献［ＦＭＹ９８］の方式では、総数ｎ個のうち、任意のｔ個の機関ＰがＲＳＡ秘密鍵ｄを算出でき、鍵回復が可能となっている。

【００３０】

【発明が解決しようとする課題】しかしながら以上のような秘密分散システムでは、以下のようにそれぞれ問題がある。文献［ＢＢＤＷ９６］の方式では、ｔ＝３におけるｎ＞3^2の場合とｔ≧４の場合には（ｔ，1^n）型の秘密分散の構築が不可であるため、（２，ｎ）型の秘密分散の構築手法が一般化されていない。

【００３１】また一方、文献［ＦＭＹ９８］の方式では、秘密鍵ｄを算出せずに、秘密鍵ｄを用いた署名や復号を試みる時には問題を生じる。例えば、公開鍵（ｅ，Ｎ）で暗号化された暗号文Ｃ＝M^e　（ｍｏｄ　Ｎ）があるとする。この暗号文Ｃを任意のｔ個の機関（この集合をΛとする）で復号するとき、各機関Ｐｊは、（６）式のようなラグランジュの補間係数$\lambda_{j,\Lambda}$を算出し、この補間係数$\lambda_{j,\Lambda}$からそれぞれ部分出力を得る必要がある。

【００３２】

【数５】

$$\lambda_{j,\Lambda} = \prod_{\ell \in \Lambda \setminus \{j\}} \frac{\ell}{\ell - j} \pmod{\phi(N)} \qquad \cdots(6)$$

【００３３】しかしながら、いずれの機関Ｐｊも合成数Ｎ（＝ｐｑ）の素因数を知らないため、巾の位数φ（Ｎ）を法とした１－ｊの乗法逆元が算出不可能となり、ラグランジュの補間係数$\lambda_{j,\Lambda}$も算出不可能となる。よって、ラグランジュの補間係数$\lambda_{j,\Lambda}$を算出時に使う部分出力が算出不可能となり、（７）式の如き、部分出力の合成により平文を復元するための分散復号が実行不可能となってしまう。

【００３４】

【数６】

$$\prod_{j \in \Lambda} C^{s_j \cdot \lambda_{j,\Lambda}} = C^d = M \pmod{N} \qquad \cdots(7)$$

【００３５】本発明は上記実情を考慮してなされたもので、分配者の無い環境で秘密鍵を算出せずに、ｎ個の機関のうち、任意ｔ個の機関による分散復号や署名を実現し得る（ｔ，ｎ）型の秘密分散システム及び記憶媒体を提供することを目的とする。

【００３６】

【課題を解決するための手段】請求項１に対応する発明は、素因数分解問題に基づく暗号系に用いられ、ｎ個の機関に秘密鍵の部分最終情報が分散され、且つ、いずれの機関も自己の部分最終情報だけでは前記秘密鍵を算出不可能な環境にあるとき、前記ｎ個の機関のうち、任意のｔ個の機関により、前記秘密鍵を算出せずに復号結果及び署名結果を生成可能な（ｔ，ｎ）型の秘密分散システムである。

【００３７】また、請求項２に対応する発明は、公開鍵及び秘密鍵ｄを用いるＲＳＡ暗号系に適用され、互いにネットワークを介して接続されたｎ個の機関及びユーザ装置を備え、ｎ個の機関に前記秘密鍵ｄの部分最終情報が分散されたとき、その中の任意のｔ個の機関により、前記秘密鍵ｄを算出せずに復号結果又は署名結果を生成可能な（ｔ，ｎ）型の秘密分散システムであって、前記ｎ個の各機関としては、前記公開鍵及び前記秘密鍵ｄを生成する手段と、この秘密鍵ｄに基づいて生成された（ｎ，ｎ）型の１個の部分情報ｄｉ（０≦ｉ≦ｎ）を保持する手段と、ｔを底としたｎの対数$\log_t n$以上の最小の整数をｒとしたとき、前記部分情報ｄｉを（ｔ，ｎ）型のｔ（ｒ＋１）個の部分乱数とし、そのうちのｒ＋１個の部分乱数を前記各機関の識別番号のｔ進表示（t^j桁目の値ｋ、０≦ｋ≦ｔ－１、０≦ｊ≦ｒ）に基づいて、それぞれ各機関に分散する手段と、前記各機関から分散されたｎ（ｒ＋１）個の部分乱数をｔ進表示の桁t^j毎にまとめてｒ＋１個の部分最終情報ｄｊ,ｋを得る手段と、前記ユーザ装置から受けた処理対象データを前記部分最終情報ｄｊ,ｋに基づいて演算処理し、得られた部分出力を前記ユーザ装置に返信する手段とを有し、前記ユーザ装置としては、前記ｔ個の機関を選択し、この選択したｔ個の各機関に処理対象データを送信する手段と、前記ｔ個の各機関から受信した部分出力を合成して前記復号結果又は署名結果を得る手段とを備えた秘密分散システムである。

【００３８】また、請求項３に対応する発明は、第１の公開鍵（ｅ，Ｎ）及び秘密鍵ｄと、第２の公開鍵（Ｌ^{2}，Ｎ）とを用いるＲＳＡ暗号系（ｅとＬ^{2}とは最大公約数が１であり、法Ｎは共通）に適用され、互いにネットワークを介して接続されたｎ個の機関及びユーザ装置を備え、ｎ個の機関に前記秘密鍵ｄの部分情報ｓｊが分散されたとき、その中の任意のｔ個の機関により、前記秘密鍵ｄを算出せずに復号結果を生成可能な（ｔ，ｎ）型の秘密分散システムであって、前記ｎ個の各機関としては、前記ユーザ装置から受けた復号対象データＣ２（＝M^{e}　（ｍｏｄＮ））を演算処理して得られた部分出力Ｚｊを前記ユーザ装置に返信する手段とを有し、前記ユーザ装置としては、前記ｎ個の機関のうちのｔ個の機関を選択し、この選択したｔ個の各機関に前記復号対象データＣ２を送信する手段と、前記ｔ個の各機関から受信した部分出力Ｚｊを合成して前記復号結果Ｃ１（＝M$^{L\hat{}2}$　（ｍｏｄ　Ｎ）、^はべき乗を示す記号）を得る手段と、前記復号結果Ｃ１、前記処理対象データＣ２及び下記式に基づいて、演算処理を実行し、最終復号結果Ｍを求める手段とを備えた秘密分散システムである。

【００３９】

a1＝（Ｌ^{2}）$^{-1}$　（ｍｏｄ　ｅ）

a2＝（a1Ｌ^{2}－１）／ｅ

Ｍ＝C_1^{a1}（C_2^{a2}）$^{-1}$　（ｍｏｄ　Ｎ）

さらに、請求項４に対応する発明は、請求項３に対応する秘密分散システムにおいて、前記復号対象データＣ２に代えて、署名対象データＳ２（＝Ｍ）を用い、前記復号結果Ｃ１に代えて、署名結果Ｓ１（＝M$^{d\ L\hat{}2}$（ｍｏｄ　Ｎ）、^はべき乗を示す記号）を用い、前記最終復号結果Ｍを求める手段に代えて、前記署名結果Ｓ１（＝（M^{d}）^{e}）、前記署名対象データＳ２（＝（M^{d}）$^{L\hat{}2}$）及び下記式に基づいて、演算処理を実行し、最終署名結果M^{d}を求める手段とを備えた秘密分散システムである。

【００４０】

a1＝（Ｌ^{2}）$^{-1}$　（ｍｏｄ　ｅ）

a2＝（a1Ｌ^{2}－１）／ｅ

M^{d}＝S_1^{a1}（S_2^{a2}）$^{-1}$　（ｍｏｄ　Ｎ）

また、請求項５に対応する発明は、公開鍵及び秘密鍵ｄを用いるＲＳＡ暗号系に適用され、互いにネットワークを介して接続されたｎ個の機関及びユーザ装置を備え、ｎ個の機関に前記秘密鍵ｄの部分最終情報が分散されたとき、その中の任意のｔ個の機関により、前記秘密鍵ｄを算出せずに復号結果又は署名結果を生成可能な（ｔ，ｎ）型の秘密分散システムに使用されるコンピュータ読み取り可能な記憶媒体であって、前記ｎ個の各機関内のコンピュータに、前記公開鍵及び前記秘密鍵ｄを生成する手段と、この秘密鍵ｄに基づいて生成された（ｎ，ｎ）型の１個の部分情報ｄｉ（０≦ｉ≦ｎ）を保持する手段と、ｔを底としたｎの対数$\log_t n$以上の最小の整数をｒとしたとき、前記部分情報ｄｉを（ｔ，ｎ）型のｔ（ｒ＋１）個の部分乱数とし、そのうちのｒ＋１個の部分乱数を前記各機関の識別番号のｔ進表示（t^{j}桁目の値ｋ、０≦ｋ≦ｔ－１、０≦ｊ≦ｒ）に基づいて、それぞれ各機関に分散する手段と、前記各機関から分散されたｎ（ｒ＋１）個の部分乱数をｔ進表示の桁t^{j}毎にまとめてｒ＋１個の部分最終情報ｄｊ,ｋを得る手段、前記ユーザ装置から受けた処理対象データを前記部分最終情報ｄｊ,ｋに基づいて演算処理し、得られた部分出力を前記ユーザ装置に返信する手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【００４１】さらに、請求項６に対応する発明は、第１の公開鍵（ｅ，Ｎ）及び秘密鍵ｄと、第２の公開鍵（Ｌ^{2}，Ｎ）とを用いるＲＳＡ暗号系（ｅとＬ^{2}とは最大公約数が１であり、法Ｎは共通）に適用され、互いにネットワークを介して接続されたｎ個の機関及びユーザ装置を備え、ｎ個の機関に前記秘密鍵ｄの部分情報ｓｊが分散されたとき、その中の任意のｔ個の機関により、前記秘密鍵ｄを算出せずに復号結果を生成可能な（ｔ，ｎ）型の秘密分散システムに使用される記憶媒体であって、前記ｎ個の各機関内のコンピュータに、前記ユーザ装置から受けた復号対象データＣ２（＝M^{e}　（ｍｏｄＮ））を演算処理して得られた部分出力Ｚｊを前記ユーザ装置に返信する手段、を実現させるためのプログラムを記憶し、前記ユーザ装置内のコンピュータに、前記ｎ個の機関のうちのｔ個の機関を選択し、この選択したｔ個の各機関に前記復号対象データＣ２を送信する手段、前記ｔ個の各機関から受信した部分出力Ｚｊを合成して前記復号結果Ｃ１（＝M$^{L\hat{}2}$（ｍｏｄ　Ｎ）、^はべき乗を示す記号）を得る手段、前記復号結果Ｃ１、前記処理対象データＣ２及び下記式に基づいて、演算処理を実行し、最終復号結果Ｍを求める手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【００４２】

a1＝（Ｌ^{2}）$^{-1}$　（ｍｏｄ　ｅ）

a2＝（a1Ｌ^{2}－１）／ｅ

Ｍ＝C_1^{a1}（C_2^{a2}）$^{-1}$　（ｍｏｄ　Ｎ）

また、請求項７に対応する発明は、請求項６に対応する記憶媒体において、前記復号対象データＣ２に代えて、署名対象データＳ２（＝Ｍ）を用い、前記復号結果Ｃ１に代えて、署名結果Ｓ１（＝M$^{d\ L\hat{}2}$（ｍｏｄ　Ｎ）、^はべき乗を示す記号）を用い、前記最終復号結果Ｍを求める手段に代えて、前記署名結果Ｓ１（＝（M^{d}）^{e}）、前記署名対象データＳ２（＝（M^{d}）$^{L\hat{}2}$）及び下記式に基づいて、演算処理を実行し、最終署名結果M^{d}を求める手段とを実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【００４３】

a1＝（Ｌ^{2}）$^{-1}$　（ｍｏｄ　ｅ）
a2＝（a1Ｌ^{2}　－１）／ｅ
Ｍ^{d}＝Ｓ$_{1}^{a1}$　（Ｓ$_{2}^{a2}$）$^{-1}$　（ｍｏｄ　Ｎ）
（作用）従って、請求項１，２，５に対応する発明は以上のような手段を講じたことにより、ｎ個の各機関が、公開鍵及び秘密鍵ｄを生成し、この秘密鍵ｄに基づいて生成された（ｎ，ｎ）型の１個の部分情報ｄｉ（０≦ｉ≦ｎ）を保持し、ｔを底としたｎの対数ｌｏｇ$_{t}$ ｎ以上の最小の整数をｒとしたとき、この部分情報ｄｉを（ｔ，ｎ）型のｔ（ｒ＋１）個の部分乱数とし、そのうちのｒ＋１個の部分乱数を各機関の識別番号のｔ進表示（ｔ^{j} 桁目の値ｋ、０≦ｋ≦ｔ－１、０≦ｊ≦ｒ）に基づいて、それぞれ各機関に分散し、各機関から分散されたｎ（ｒ＋１）個の部分乱数をｔ進表示の桁ｔ^{j} 毎にまとめてｒ＋１個の部分最終情報ｄｊ,ｋ を得る。
【００４４】続いて、ユーザ装置が、ｔ個の機関を選択し、この選択したｔ個の各機関に処理対象データを送信し、ｔ個の機関が、ユーザ装置から受けた処理対象データを部分最終情報ｄｊ,ｋ に基づいて演算処理し、得られた部分出力をユーザ装置に返信し、ユーザ装置が、ｔ個の各機関から受信した部分出力を合成して復号結果又は署名結果を得る。
【００４５】このように、分配者の無い環境で秘密鍵を算出せずに、ｎ個の機関のうち、任意ｔ個の機関による分散復号や署名を実現することができ、また、ラグランジュ補間法を用いず、高い処理効率を実現することができる。
【００４６】また、請求項３，６に対応する発明は、第１の公開鍵（ｅ，Ｎ）及び秘密鍵ｄと、第２の公開鍵（Ｌ^{2}，Ｎ）とを用いるＲＳＡ暗号系（ｅとＬ^{2} とは最大公約数が１であり、法Ｎは共通）において、ｎ個の機関に秘密鍵ｄの部分情報ｓｊ が分散されたとき、ユーザ装置が、ｎ個の機関のうちのｔ個の機関を選択し、この選択したｔ個の各機関に復号対象データＣ２を送信し、ｔ個の各機関が、ユーザ装置から受けた復号対象データＣ２（＝Ｍ^{e}　（ｍｏｄ　Ｎ））を演算処理して得られた部分出力Ｚｊ をユーザ装置に返信し、ユーザ装置が、ｔ個の各機関から受信した部分出力Ｚｊ を合成して復号結果Ｃ１（＝Ｍ$^{L\hat{}2}$　（ｍｏｄ　Ｎ））を得ると共に、復号結果Ｃ１、処理対象データＣ２及び所定の式（a1＝（Ｌ^{2}）$^{-1}$（ｍｏｄ　ｅ）、a2＝（a1Ｌ^{2}　－１）／ｅ、Ｍ＝Ｃ$_{1}^{a1}$　（Ｃ$_{2}^{a2}$）$^{-1}$　（ｍｏｄ　Ｎ））に基づいて、演算処理を実行し、最終復号結果Ｍを求める。
【００４７】これにより、分配者の無い環境で秘密鍵を算出せずに、ｎ個の機関のうち、任意ｔ個の機関による分散復号を実現することができ、また、所定条件の公開鍵を用いたラグランジュ補間法に基づき、高い確実性を実現することができる。
【００４８】さらに、請求項４，７に対応する発明は、前記復号対象データＣ２に代えて、署名対象データＳ２（＝Ｍ）を用い、復号結果Ｃ１に代えて、署名結果Ｓ１（＝Ｍ$^{d\ L\hat{}2}$（ｍｏｄ　Ｎ）、＾はべき乗を示す記号）を用い、最終復号結果Ｍを求める手段に代えて、署名結果Ｓ１（＝（Ｍ^{d}）^{e}）、署名対象データＳ２（＝（Ｍ^{d}）$^{L\hat{}2}$）及び所定の式（a1＝（Ｌ^{2}）$^{-1}$　（ｍｏｄ　ｅ）、a2＝（a1Ｌ^{2}　－１）／ｅ、Ｍ^{d}＝Ｓ$_{1}^{a1}$　（Ｓ$_{2}^{a2}$）$^{-1}$　（ｍｏｄ　Ｎ））に基づいて、演算処理を実行し、最終署名結果Ｍ^{d} を求める。
【００４９】これにより、請求項３，６に対応する作用と同様の作用を署名処理において実現することができる。
【００５０】
【発明の実施の形態】次に、本発明の各実施形態について図面を参照して説明する。なお、第１の実施形態は、ラグランジュ補間法を用いず、高い処理効率を実現したものであり、第２の実施形態は、所定条件の公開鍵を用いたラグランジュ補間法に基づき、高い確実性を実現したものであって、両者ともノンディーラーモデルのしきい値法による分散復号及び署名の可能な（ｔ，ｎ）型の秘密分散システムとなっている。以下、順次説明する。
【００５１】（第１の実施形態）本実施形態は、文献［ＢＦ９７］における（２，２）型から（２，ｎ）型の秘密分散を構築する方式を一般化した（ｔ，ｎ）型の秘密分散システムである。具体的には、文献［ＢＦ９７］の方式を用いて各機関Ｐｉ が秘密鍵ｄの（ｎ，ｎ）型の部分情報ｄｉ を保持すると、全ての機関Ｐ１ ～Ｐｎ がそれぞれ部分情報ｄｉ を（ｔ，ｎ）型の部分乱数情報として分配し、各機関Ｐ１ ～Ｐｎ が部分乱数情報を桁毎にまとめて複数の部分情報ｄｊ,ｋ を得る（ｔ，ｎ）型の秘密分散システムとなっている。
【００５２】図１は本発明の第１の実施形態に係る秘密分散システムの構成を示す模式図である。この秘密分散システムは、各々計算機システムとしてのｎ個の機関Ｐ１ ～Ｐｎ 及びユーザ装置Ｕが互いにネットワークを介して接続されている。
【００５３】なお、各機関Ｐ１ ～Ｐｎ は、互いに同一構成を有するので、ここでは任意の機関Ｐｉ （但し、１≦ｉ≦ｎ）を代表例として説明する。
【００５４】機関Ｐｉ は、公開鍵（ｅ，Ｎ）及び秘密鍵ｄを生成する機能と、［ＢＦ９７］の方式に基づいて、秘密鍵ｄを（２，ｎ）型の部分情報とし、そのうちのｒ＋１個の部分情報をそれぞれ各機関Ｐ１ ～Ｐｎ に分散する機能と、分散されたｒ＋１個の部分情報に基づいて、（ｎ，ｎ）型の１個の部分情報ｄｉ を保持する機能と、この部分情報ｄｉ を（ｔ，ｎ）型の部分乱数とし、そのうちのｒ＋１個の部分乱数を機関の識別番号のｔ進表示に基づいて、それぞれ各機関Ｐ１ ～Ｐｎ に分散する機能と、各機関Ｐ１ ～Ｐｎ から分散されたｎ（ｒ＋１）個の部分乱数をｔ進表示の桁ｔ^{j} 毎にまとめてｒ＋１個の部分情報ｄｊ,ｋ を得る機能と、ユーザ装置Ｕから受けた暗

号文Ｃを復号処理して得られた部分出力Ｘｚ をユーザ装置Ｕに返信する機能とをもっている。

【００５５】また、各機関Ｐｉ は、任意のｔ個が選択された場合、図示しないが、“Ｐ”に代えて“Ｔ”の表記を用いる。例えば“機関Ｐｚ ”は選択されているとき、“機関Ｔｚ ”と表記される。

【００５６】ユーザ装置Ｕは、ｎ個の機関Ｐ１ ～Ｐｎ のうちのｔ個の機関Ｔｚ を選択する機能と、公開鍵（ｅ，Ｎ）で暗号化された暗号文Ｃをｔ個の各機関Ｔｚ に送信する機能と、各機関Ｔｚ から受信した部分出力Ｘｚ を合成して平文Ｍを得る機能とをもっている。

【００５７】次に、各機関Ｐ１ ～Ｐｎ 及びユーザ装置Ｕの具体的なハードウェア構成について述べる。具体的には、機関Ｐｉ 及びユーザ装置Ｕは、ハードウェア的には図２に示すように、ＣＰＵ１１、コントローラ１２、メモリ１３、通信デバイス１４、ディスプレイ１５、キーボード１６及びプリンタ１７が互いにバス１８を介して接続された計算機システムである。

【００５８】これらの構成のうち、メモリ１３は、いわゆる主記憶（ＲＡＭ等）と二次記憶装置（ハードディスク等）の双方を含むものである。この主記憶上に読み込まれたプログラムと、このプログラムに従うＣＰＵ１１の制御とにより、機関Ｐｉ が行うべき機能が実現される。すなわち、各機関Ｐ１ ～Ｐｎ 及びユーザ装置Ｕは、ソフトウェア的には、上述したそれぞれの機能を行うように、互いに異なる構成を有するものである。これらハードウェア及びソフトウェアの結合からなるそれぞれの機能の詳細な内容は、以下の動作説明において詳細に述べる。

【００５９】但し、各機関Ｐ１ ～Ｐｎ は、ユーザ装置Ｕから受信したデータを演算処理し、結果をユーザ装置Ｕに返信するためのハードウェアがあればよいので、例えばディスプレイ１５、キーボード１６及びプリンタ１７などを適宜、省略してもよい。同様に、ユーザ装置Ｕにおいても、例えばプリンタ１７を省略してもよい。

【００６０】次に、以上のように構成された秘密分散システムの動作を説明する。

（（ｔ，ｎ）型の秘密分散）各機関Ｐ１ ～Ｐｎ は、公開鍵（ｅ，Ｎ）及び秘密鍵ｄを生成すると、文献［ＢＦ９７］の方式に基づいて、秘密鍵ｄを（２，ｎ）型の部分情報とし、そのうちのｒ＋１個の部分情報をそれぞれ各機関Ｐ１ ～Ｐｎ に分散する。

【００６１】各機関Ｐ１ ～Ｐｎ は、［ＢＦ９７］の方式によるｒ＋１個の部分情報に基づき、合成数Ｎにおける互いに異なる２つの素因数ｐ，ｑと、秘密鍵ｄとを（ｎ，ｎ）型で秘密共有している。

【００６２】すなわち、各機関Ｐｉ （１≦ｉ≦ｎ）は、図３に示すように、次の（８）式を満たす部分情報ｄｉをそれぞれ保管している（ＳＴ１）。

【００６３】ｄ＝ｄ１ ＋ｄ２ ＋…＋ｄｎ　　…（８）

次に、全ての各機関Ｐｉ は、自己の部分情報ｄｉ のディーラーとして機能する。すなわち、全ての各機関Ｐｉ は、（９）式に示すように、自己の部分情報ｄｉを示す（ｔ，ｎ）型の部分乱数情報Ｓｊ，１（０≦ｊ ≦ｒ，０≦１≦ｔ－２）を生成する（ＳＴ２）。但し、ｒ＝「１ｏｇｔ ｎ」である。

【００６４】

【数７】

$$S_{j,t-1}^{(i)} = d_i + \sum_{\ell=0}^{t-2} S_{j,\ell} \qquad \cdots(9)$$

【００６５】なお、この部分乱数情報Ｓｊ，１の生成処理は、全ての各機関Ｐｉ が、それぞれ次に示す如き、自己の部分情報ｄｉ を示すｒ＋１個の独立多項式を作成することと等価である。

【００６６】

$$\begin{aligned} d_i &= S_{0,0} + S_{0,1} + \cdots + S_{0,t-2} + S_{0,t-1} \\ &= S_{1,0} + S_{1,1} + \cdots + S_{1,t-2} + S_{1,t-1} \\ &= \cdots \\ &= S_{j,0} + S_{j,1} + \cdots + S_{j,t-2} + S_{j,t-1} \\ &= \cdots \\ &= S_{r,0} + S_{r,1} + \cdots + S_{r,t-2} + S_{r,t-1} \end{aligned}$$

次に、全ての各機関Ｐｉ は、識別番号をｚとしたとき、以下のステップＳＴ３～ＳＴ４に示すように、各機関Ｐｚ （１≦ｚ≦ｎ）と互いに部分乱数情報$S_{j,1}$を分散しあう。すなわち、機関Ｐｚの識別番号ｚを（１０）式に示すように、ｔ進数に変換する（ＳＴ３）。

$$z = \beta_{r,z}\, t^{r} + \beta_{r-1,z}\, t^{r-1} + \cdots + \beta_{j,z}\, t^{j} + \cdots + \beta_{0,z} \qquad \cdots(10)$$

簡単のため、（１０）式を（１１）式のように表記する。

$$z(t) = \beta_{r,z} \quad \beta_{r-1,z} \quad \cdots \quad \beta_{j,z} \quad \cdots \quad \beta_{0,z} \qquad \cdots(11)$$

但し、ｔ進値$\beta_{r,z}$　{０，…，t-1 }

また、各機関Ｐｉ は、ｚ（ｔ）における各桁t^{j} 毎のｔ進値βに基づいて、次に示すｒ＋１個の部分乱数情報を含む集合Ｓを機関Ｐｚに送信する（ＳＴ４）。

【００６７】

【数８】

$$(S_{r,\beta r,z}^{(i)}, S_{r-1,\beta r-1,z}^{(i)}, \cdots, S_{0,\beta 0,z}^{(i)})$$

【００６８】各機関Ｐｚ は、自己を含む全ての各機関Ｐｉ から得た集合Ｓに基づいて、次の（１２）式に示すように、各桁j 毎の部分乱数情報Ｓｊ,１ の総和をとって部分情報ｄｊ,ｋ を算出する（ＳＴ５）。但し、ｋ　{$\beta_{r,z}$　$\beta_{r-1,z}$　…　$\beta_{0,z}$ }，０≦ｊ≦ｒである。

【００６９】
【数９】

$$d_{j,k} = \sum_{i=1}^{n} S_{j,k}^{(i)} = S_{j,k}^{(1)} + S_{j,k}^{(2)} + \cdots + S_{j,k}^{(n)} \qquad \cdots(12)$$

【００７０】各機関Ｐｚ は、桁ｊ の数に対応するｒ＋１個の部分情報ｄｊ,ｋ を保管する（ＳＴ６）。なお、部分情報ｄｊ,ｋ は、秘密鍵ｄの部分集合である。

【００７１】秘密鍵ｄと部分秘密鍵ｄｊ,ｋ との関係は、以下の（１３）式に示す通りである。

$$\begin{aligned} d &= d_{0,0} + d_{0,1} + \cdots + d_{0,t-1} && (t^0 \text{ 桁目}) \\ &= d_{1,0} + d_{1,1} + \cdots + d_{1,t-1} && (t^1 \text{ 桁目}) \\ &= \quad \cdots && (\ \cdots\ ) \\ &= d_{r,0} + d_{r,1} + \cdots + d_{r,t-1} && (t^r \text{ 桁目}) \end{aligned} \qquad \cdots(13)$$

例えば、（３，２７）型の秘密分散における機関ｚ＝２０の保管情報は、以下の通りである。

【００７２】

$r = \lfloor \log_3 27 \rfloor = 3$

$20 = 0\times3^3 + 2\times3^2 + 0\times3^1 + 2\times3^0$

$20(3) = 0202$　（３進表示）

$$\begin{aligned} d &= d_{3,0} + d_{3,1} + d_{3,2} && (3^3 \text{ 桁目}) \\ &= d_{2,0} + d_{2,1} + d_{2,2} && (3^2 \text{ 桁目}) \\ &= d_{1,0} + d_{1,1} + d_{1,2} && (3^1 \text{ 桁目}) \\ &= d_{0,0} + d_{0,1} + d_{0,2} && (3^0 \text{ 桁目}) \end{aligned} \qquad (14)$$

よって、機関P_{20}は、次の（１４）式に示す全ての部分情報のうち、識別番号ｚの３進表示(0202)に対応する部分情報（$d_{3,0}$，$d_{2,2}$，$d_{1,0}$，$d_{0,2}$）を保管する。

【００７３】（分散復号化）ｎ個の機関Ｐ１ ～Ｐｎ のうち、任意のｔ個の機関Ｔｚ （この集合をΛとする）は、ユーザ装置Ｕからの復号依頼により、ユーザ装置Ｕの公開鍵（ｅ，Ｎ）で暗号化されたデータＣ＝M^e （ｍｏｄ　Ｎ）を図４のステップＳＴ１１～ＳＴ１６に示すように分散復号化する。

【００７４】すなわち、ユーザ装置Ｕは、（１５）式に示すように、ｔ個の機関Ｔｚ の識別番号ｚをそれぞれｔ進表示に変換する（ＳＴ１１）。

【００７５】

$$z(t) = \beta_{r,z} \quad \beta_{r-1,z} \quad \cdots \quad \beta_{0,z} \qquad \cdots(15)$$

続いて、ユーザ装置Ｕは、ｔ個の機関Ｔａ，Ｔｂ　Λ（ａ≠ｂ）におけるｔ進表示の各桁t^j（０≦ｊ≦ｒ）毎に、ｔ進表示の値βが全て異なる（$\beta_{j,a} \neq \beta_{j,b}$）という条件を満たす桁$t^j$が有るか否かを判定する（ＳＴ１２）。

【００７６】この条件を満たす桁t^jがないとき、この集合Λによる分散復号は不可能であるため、集合Λ内の機関Ｔｚを多少入れ換えて（ＳＴ１３）、ステップＳＴ１１から再実行する。

【００７７】ステップＳＴ２で条件を満たす桁t^jがあるとき、ユーザ装置Ｕは、暗号化データＣを各機関Ｔｚに送信する（ＳＴ１４）。

【００７８】各機関Ｔｚ は、t^j 桁に対応する部分情報ｄｊ,ｋ （ｋ＝βｊ,ｚ ）に基づいて、暗号化データＣを復号処理し、得られた部分出力Ｘｚ （＝$C^{dj,k}$　（ｍｏｄ　Ｎ））をそれぞれユーザ装置Ｕに返信する（ＳＴ１５）。

【００７９】ユーザ装置は、ｔ個の各機関Ｔｚ （ｚ　Λ）から受信したｔ個の部分出力Ｘｚ（ｚ　Λ）を（１６）式のように合成し、平文Ｍを復元することができる（ＳＴ１６）。

$$\begin{aligned} \prod_{z\in\Lambda} &= C^{d_{j,1}} C^{d_{j,2}} \cdots C^{d_{j,t}} \\ &= (M^e)^{d_{j,1}+d_{j,2}+\cdots+d_{j,t}} \\ &= (M^e)^d \\ &= M \pmod N \end{aligned} \qquad \cdots(16)$$

【００８０】
【数１０】

【００８１】また、以上の動作は、暗号化データＣ（＝M^e （ｍｏｄ　Ｎ））をｔ個の各機関Ｔｚに送ることにより、平文Ｍを分散復号した場合である。これに限らず、本実施形態は、図５に示すように、暗号化データＣに代えて、署名対象データＭをｔ個の各機関Ｔｚに送信したとき（ＳＴ１４ａ）、前述した部分出力Ｘｚの合成により、署名M^d （ｍｏｄ　Ｎ）を得ることもできる（ＳＴ１６ａ）。上述したように本実施形態によれば、ｎ個の各機関Ｐ１ ～Ｐｎ が、公開鍵及び秘密鍵ｄを生成し、この秘密鍵ｄに基づいて生成された（ｎ，ｎ）型の１個の部分情報ｄｉ （０≦ｉ ≦ｎ）を保持し、ｔを底としたｎの対数$\log_t$ ｎ以上の最小の整数をｒとしたとき、この部分情報ｄｉ を（ｔ，ｎ）型のｔ（ｒ＋１）個の部分乱数Ｓｊ とし、そのうちのｒ＋１個の部分乱数Ｓｊ を各機関Ｐｉの識別番号ｚのｔ進表示（t^j 桁目の値ｋ、０≦ｋ ≦ｔ－１、０≦ｊ ≦ｒ）に基づいて、それぞれ各機関Ｐ１ ～Ｐｎ に分散し、これら分散されたｎ（ｒ＋１）個の部分乱数をｔ進表示の桁t^j 毎にまとめてｒ＋１個の部分情報ｄｊ,ｋ を得る。

【００８２】続いて、ユーザ装置Ｕが、ｔ個の機関Ｔｚを選択して暗号化データＣ（又は署名対象データ）を送信し、ｔ個の機関Ｔｚが、暗号化データＣ（又は署名対象データ）を部分情報ｄj,k に基づいて演算処理し、得られた部分出力Ｘｚをそれぞれユーザ装置Ｕに返信し、ユーザ装置Ｕが、ｔ個の部分出力Ｘｚを合成して復号結果（又は署名結果）を得る。

【００８３】このように、分配者の無い環境で秘密鍵を算出せずに、ｎ個の機関のうち、任意ｔ個の機関による分散復号や署名を実現することができる。また、復号分散時に、ラグランジュの補間係数を算出する手間を省略でき、高い処理効率を実現することができる。

【００８４】また、本実施形態は、予め暗号文への入力を表として保持でき、ラグランジュの補間係数の算出が不要な分だけ、文献［ＦＭＹ９８］の方式よりも、演算の処理効率を向上させることができる。

【００８５】さらに、本実施形態は、全ての組合せに応じたラグランジュの補間係数を表として保管する場合、文献［ＦＭＹ９８］の方式よりも、保管する情報の量を低減させることができる。

【００８６】例えば、文献［ＦＭＹ９８］の方式は、ラグランジュの補間法に基づくしきい値法を用いた分散復号化を行う。ここでは、秘密鍵ｄが各機関Ｐ1 ～Ｐn のもつ部分情報の単純和ではなく、各機関Ｐj は、前述したラグランジュの補間係数$\lambda_{j,\Lambda}$を算出し、合成する必要がある。よって、補間係数$\lambda_{j,\Lambda}$を予め算出して表に保管する場合、１つの部分情報と参加機関Ｔz の全ての組合せに応じた${}_nC_t$ 個の補間係数$\lambda_{j,\Lambda}$を算出して保管する必要がある。

【００８７】一方、本実施形態では、「$\log_t n$」＋１個の部分情報から機関の組合せに対応する部分情報を選択すればよい。よって、保管される部分情報は、「$\log_t n$」＋１個でよく、少ない情報量となっている。

【００８８】ところで、本実施形態の方式によれば、ｔ個の機関の組合せが悪いとき、暗号文を分散復号できない場合がある。この場合について（３，２７）型の秘密分散を例に挙げて補足的に説明する。今、秘密鍵ｄについて、以下のｒ＋１個の多項式が成立しているとする。

【００８９】

$$d=d_{3,0}+d_{3,1}+d_{3,2}\quad(3^3\text{ 桁目})$$
$$=d_{2,0}+d_{2,1}+d_{2,2}\quad(3^2\text{ 桁目})$$
$$=d_{1,0}+d_{1,1}+d_{1,2}\quad(3^1\text{ 桁目})$$
$$=d_{0,0}+d_{0,1}+d_{0,2}\quad(3^0\text{ 桁目})$$

まず、分散復号が可能な場合を示す。２７個の機関のうち、機関P_{20}，P_{23}，P_{26}が分散復号プロトコルに介入するとき、復号操作$C^d=M^{ed}=M$は成功する。ここで、各機関P_{20}，P_{23}，P_{26}の３進表示は、P_{20}＝０２０２，P_{23}＝０２１２，P_{26}＝０２２２であり、それぞれの保管情報は図６に示す通りとなっている。ここで、3^1 桁に注目すると、（１７）式に示すように、$d=d_{1,0}+d_{1,1}+d_{1,2}$ からｄによる復号化処理が可能となる。

$$C^{d_{1,0}}\cdot C^{d_{1,1}}\cdot C^{d_{1,2}}=M^{ed}=M\pmod N\qquad\cdots(17)$$

ところが、P_{23}に代えてP_{11}を用いた各機関P_{20}，P_{23}，P_{11}では、復号操作は失敗する。すなわち、各機関の３進表示は、P_{20}＝０２０２，P_{23}＝０２１２，P_{11}＝０１０２であり、それぞれの保管情報は図７に示す通りである。

【００９０】この場合、秘密鍵ｄを構成する３つの部分情報（$d_{j,0}+d_{j,1}+d_{j,2}$）がどの桁j でも揃わず、いずれかの部分情報が２つ以上の機関において重複（衝突）している。このように保管する部分情報の重複により、分散復号の不可能な場合がある。

【００９１】この場合、別のｔ個の機関を選択し直す必要がある。ここで、機関の総数ｎが大きく、ｔ個以上の機関を比較的自由に選択可能な場合、本実施形態の（ｔ，ｎ）型の秘密分散が適している。すなわち、機関の総数ｎが大きいときには復号不能となっても、ｔ個の機関Ｐを再編成して分散復号プロトコルをし直せばよい。

【００９２】逆にｎの数が小さく、機関Ｐの選択の余地がない場合は、全ての組合せに応じた関係式を作成する方式が適している。例えば、エルガマル(ElGamal) 暗号系では、ｎ個のうちの任意のｔ個の機関がグループの鍵で暗号化された暗号文を復号することができる技術が提案されている（T. P. Pedersen, A threshold cryptosystem without a trusted party, Advances in Cryptology-Eurocrypt 91, LNCS 547, pp.522-526, 1991.（以下、文献［Ｐｅｄ９１ｂ］という））。すなわち、文献［Ｐｅｄ９１ｂ］の方式のように任意のｔ個の機関で分散復号・鍵復元を行うには、秘密鍵ｄに関する${}_nC_t$ 個の独立な関係式を作成すればよい。具体的には、ある組合せ（Λ）のときは（１８）式のように該当する関係式により分散復号を行う方式である。

【００９３】

$$d=d_{1,\Lambda}+d_{2,\Lambda}+\cdots+d_{t,\Lambda}\qquad\cdots(18)$$

しかしながら、文献［Ｐｅｄ９１ｂ］の方式では、衝突の可能性はないものの、機関の総数ｎに比例して関係式の数が膨大になってしまう。よって、衝突の可能性の低い範囲で、独立多項式を最小限に抑えることが好ましい。

【００９４】各方式はそれぞれ長所・短所があるので、第１実施形態の方式（再編成する方式）、第１実施形態の方式において関係式を用いる方式、あるいは後述する第２の実施形態の方式（補間法を用いる方式）のいずれを選択するかは、機関の総数ｎや処理効率、使用される環境、復号処理不能が許されるか否かなどの条件に応じ

て使い分けることが好ましい。

【００９５】（第２の実施形態）次に、本発明の第２の実施形態について説明するが、その前に本実施形態の前提となるＲＳＡ共通法誤用プロトコルについて述べる。

【００９６】ＲＳＡ暗号系において、１つのメッセージＭを、互いに共通する法Ｎと、互いに異なる公開指数e1，e2とを用いる条件の下でそれぞれ暗号化し、得られた２つの異なる暗号文C_1，C_2があるとする。この場合、合成数Ｎの素因数が不明でも、２つの暗号文C_1，C_2からメッセージＭを復元できる（G. J. Simmons, A weak privacy protocol using the RSA cryptoalgolithm, Cryptologia, vol.7, pp.180-182, 1983.（以下、文献［Ｓｉｍ８３］という））。

【００９７】この文献［Ｓｉｍ８３］の方式において、前述した２つの暗号文C_1，C_2は、次の（１９）式～（２０）式に示すように得られている。

【００９８】

$C_1 = M^{e1} \pmod N$　　…（１９）

$C_2 = M^{e2} \pmod N$　　…（２０）

ここで、異なる公開指数e1,e2 の最大公約数gcd（e1, e2）＝１である場合、以下のステップＳＴc1～ＳＴc3を行うと、２つの暗号文C_1，C_2からメッセージＭを復元できる（D. R. Stinson, CRYPTOGRAPHY : Theory and Practice, CRCPress, Inc. Boca Raton, Florida, U.S.A., 1995.（以下、文献［Ｓｔｉ９５］という））。

【００９９】

（ステップＳＴc1）$a1 = e1^{-1} \pmod{e2}$

（ステップＳＴc2）$a2 = (a1e1 - 1) / e2$

（ステップＳＴc3）$M = C_1^{a1} (C_2^{a2})^{-1} \pmod N$

また、上記処理（Step c1 ～c3）を次のように表記する。

【０１００】Common（e1, e2）→Ｍ

以上のように、ＲＳＡ暗号系においては、所定の条件を満たすとき、メッセージＭを復元可能なプロトコルが存在する。このプロトコルがＲＳＡ共通法誤用プロトコルと呼ばれている。

【０１０１】さて次に、本発明の第２の実施形態に係る秘密分散システムについて説明する。本実施形態は、文献［Ｓｉｍ８３］及び［Ｓｔｉ９５］等のＲＳＡ共通法誤用プロトコルを適用可能な条件で公開鍵を作成し、文献［ＦＭＹ９８］の手法により、秘密鍵ｄの部分情報ｓｊを分散する（ｔ，ｎ）型の秘密分散システムである。

【０１０２】なお、ＲＳＡ共通法誤用プロトコルを適用可能な条件とは、次の（ａ）～（ｃ）を全て満たすことに相当する。

（ａ）メッセージＭが同じである。

（ｂ）法Ｎが共通する。

（ｃ）互いに異なる公開指数（e1, e2）の最大公約数gcd（e1, e2）＝１である。但し、以下の説明では、公開指数（e1, e2）を（L^2，ｅ）と表記している。また、公開指数L^2の元となるＬは、Ｌ＝ｎ！に代えて、Ｌ＝（ｎ－１）！としてもよい。また、ユーザ装置及び各機関は、ハードウェア的な構成に関しては図１及び図２に示した通りとし、機能に関しては第１実施形態とは異なるので、以下に説明する。

【０１０３】なお、各機関Ｐ1 ～Ｐn は、前述同様に、任意の機関Ｐi （但し、１ ≦i ≦n）を代表例として説明する。機関Ｐi は、［ＦＭＹ９８］の方式に基づいて、法Ｎの部分情報（ｐｊ，ｑj）を作成する機能と、これら部分情報ｐｊ，ｑj をそれぞれ各機関Ｐ1 ～Ｐn に分散する機能と、各機関Ｐj の（ｐｊ，ｑｊ）を基に、公開鍵（ｅ，Ｎ）を生成する機能と、秘密鍵ｄから（ｔ，ｎ）型の部分情報ｓｊを得る機能と、夫々部分情報（ｐｊ，ｑj）及びｓj を保持する機能と、ユーザから受けた暗号文Ｃ（＝$C_2 = M^e \pmod N$）を復号処理して得られた部分出力Ｚj をユーザ装置Ｕに返信する機能とをもっている。

【０１０４】ユーザ装置Ｕは、ｎ個の機関のうちのｔ個の機関Ｔz を選択する機能と、公開鍵（ｅ，Ｎ）で暗号化された暗号文C_2（$= M^e \pmod N$）をｔ個の各機関Ｔz に送信する機能と、各機関Ｔz から受信した部分出力Ｚj を合成して暗号文C_1（$= M^{L2} \pmod N$）を得る機能と、２つの暗号文（M^{L2}, M^e）から、前述したＲＳＡ共通法誤用プロトコルCommon（L^2，ｅ）→Ｍを用いて、メッセージＭを算出する機能とをもっている。

【０１０５】次に、以上のように構成された秘密分散システムの動作を説明する。

（（ｔ，ｎ）型の秘密分散）各機関は互いに、文献［ＦＭＹ９８］の方式に基づいて、秘密鍵ｄを（ｔ，ｎ）型の部分情報とし、対応する部分情報ｓj を個別にｎ個の機関Ｐ1 ～Ｐn に分散する。

【０１０６】具体的には、各機関Ｐj は、法Ｎの構成要素（ｐｊ，ｑｊ）を作成し、夫々送信する。各機関Ｐj は、他の各機関Ｐj から受けた（ｐｊ，ｑｊ）の合成Ｎ＝（ｐ1 ＋ｐ2 ＋…＋ｐn ）（ｑ1 ＋ｑ2 ＋…＋ｑn ）が異なる２つの素数の積であるか否かを判定し、異なる素数の積であるとき、正当として次に進む。

【０１０７】各機関Ｐj は（ｐｊ，ｑｊ）を基に、公開鍵（ｅ，Ｎ）を生成し、各機関Ｐjの保持すべき秘密鍵ｄの部分情報ｄj を算出する（（ｎ，ｎ）型秘密分散完了）。

【０１０８】ｄ＝ｄ1 ＋ｄ2 ＋…＋ｄj ＋…＋ｄn

次に、各機関Ｐj は、（ｎ，ｎ）型の秘密鍵ｄをSum-to-Poly の技術により、（ｔ，ｎ）型の秘密鍵ｄに変換する（（ｔ，ｎ）型秘密分散完了）。

【０１０９】このとき、ｔ－１個の乱数 {b1, …b_{t-1}} Ｚに対し、（２１）式の如き、多項式を定める。

$$f(x) = d + b1x + b2x^2 + \cdots + b_{t-1}x^{t-1} \quad \cdots(21)$$

この式は、ｙ切片を秘密鍵ｄとしたｋ－１次の多項式であり、ラグランジュの補間法により、ｋ個の座標点（ｊ，ｆ(ｊ)）から一意に定まる性質をもっている。但し、ｋ－１個の座標点からは一意に定まらず、任意のｙ切片が可能となり、秘密鍵ｄを得られない性質もある。

【０１１０】各機関Ｐｊは、各機関Ｐ１～Ｐｎの自己の識別番号ｊ（１≦ｊ≦ｎ）を独立変数ｘとして上記多項式ｆ(ｘ)に代入してｆ(ｊ)を計算し、ｆ(ｘ)上のｙ座標を示す部分情報ｓｊ（＝ｆ(ｊ)）を各機関Ｐｊ毎に得る。

【０１１１】各機関Ｐｊは、得られた（ｔ，ｎ）型の部分情報ｓｊと、予め保持する、法Ｎの素因数ｐｑの部分情報（ｐｊ，ｑｊ）とを保管する。なお、（ｎ，ｎ）型の部分情報ｄｊも保持されるが、本実施形態では特に使用されない。

【０１１２】（分散復号化）ｎ個の機関のうち、任意のｔ個の機関Ｔｚ（この集合をΛとする）は、ユーザ装置Ｕからの復号依頼により、ユーザ装置Ｕの公開鍵（ｅ，Ｎ）で暗号化されたデータＣ＝M^e（ｍｏｄ　Ｎ）を図８のステップＳＴ２１～ＳＴ２４に示すように分散復号化する。ここで、Ｌ＝ｎ！かつ最大公約数gcd（ｅ，L^2）＝１とする。

【０１１３】すなわち、ユーザ装置Ｕは、暗号文Ｃ（＝M^e　（ｍｏｄ　Ｎ））をｔ個の各機関Ｔｊ（　Λ）に送信する（ＳＴ２１）。各機関Ｔｊは、次の（２２）式～（２４）式の通り、それぞれ自己の部分情報ｓｊを用いて部分出力Ｚｊを算出し、得られた部分出力Ｚｊをユーザ装置Ｕに返信する（ＳＴ２２）。

【０１１４】

【数１１】

$$\lambda_{j,\Lambda} = \prod_{\ell \in \Lambda \setminus \{j\}} \frac{\ell}{\ell - j} \quad \cdots(22)$$

$$\sigma_j = s_j \cdot L^2 \cdot \lambda_{j,\Lambda} \quad \cdots(23)$$

$$Z_j = C^{\sigma_j} \pmod N \quad \cdots(24)$$

【０１１５】ユーザ装置Ｕは、次の（２５）式のように、ｔ個の各機関Ｔｊから受ける部分出力Ｚｊを合成し、暗号文M^{L^2}（ｍｏｄ　Ｎ）を算出する（ＳＴ２３）。

【０１１６】

【数１２】

$$\prod_{j\in\Lambda} Z_j = (M^e)^{L^2 \cdot \sum_{j\in\Lambda}(s_j \cdot \lambda_{j,\Lambda})} = M^{L^2} \pmod N \quad \cdots(25)$$

【０１１７】ユーザ装置Ｕは、元の暗号文M^eと、この暗号文M^{L^2}との互いに異なる２つの暗号文（M^{L^2}，M^e）から、前述したＲＳＡ共通法誤用プロトコルCommon（L^2，ｅ）→Ｍを用いて、メッセージＭを算出する（ＳＴ２４）。なお、本実施形態と、前述したプロトコルとの対応関係は、（M^{L^2}，M^e）＝（C_1，C_2）であり、（L^2，ｅ）＝（e1，e2）である。ここで、ＲＳＡ共通法誤用プロトコルは、（２６）式に示すように、健全性を有している。

【０１１８】

$$C1^{a1} \ (C2^{a2})^{-1} = M^{L^2 a1 - e a2} = M \ (\mathrm{mod}\ N) \quad \cdots(26)$$

（分散署名）なお、ユーザ装置Ｕは、分散復号に限らず、ｔ個の機関Ｔｚに分散署名を行わせてもよい。この場合、ユーザ装置Ｕは、図９に示すように、復号対象の暗号文Ｃに代えて、署名対象データＳ１（＝Ｍ）を用い（ＳＴ２１ａ）、復号結果の暗号文M^{L^2}に代えて、署名結果Ｓ２（＝$(M^d)^{L^2}$（ｍｏｄ　Ｎ）、^はべき乗を示す記号）を用いる（ＳＴ２３ａ）。

【０１１９】そして、ユーザ装置Ｕは、（C_1，C_2）＝（M^{dL^2}，Ｍ）＝（$(M^d)^{L^2}$，$(M^d)^e$）から、

$$C1^{a1} \ (C2^{a2})^{-1} = M^{d(L^2 a1 - e a2)} = M^d \ (\mathrm{mod}\ N) \quad \cdots(27)$$

（分散署名の変形例）なお、上述した分散署名は、図１０に示すように変形してもよい。すなわち、ステップＳＴ２３ａの後、ユーザ装置Ｕは、この署名対象データＳ１及び署名結果Ｓ２の組を図示しない相手先の署名検証装置に送信する（ＳＴ２５ａ）。署名検証装置は、署名対象データＳ１及び第１公開鍵（ｅ，Ｎ）から第１比較データＤ１（＝M^e　（ｍｏｄ　Ｎ））を算出し、署名結果Ｓ２及び第２公開鍵（ｅ，Ｎ）から第２比較データＤ２（＝M^{L^2}　（ｍｏｄ　Ｎ））を算出する（ＳＴ２６ａ）。

【０１２０】

$a1 = (L^2)^{-1} \ (\mathrm{mod}\ e)$

$a2 = (a1L^2 - 1)/e$

$M = C_1^{a1} \ (C_2^{a2})^{-1} \ (\mathrm{mod}\ N)$

ここで、ＲＳＡ共通法誤用プロトコルは、（２７）式に示すように、健全性を有している。

【０１２１】

前述同様に、以下のＲＳＡ共通法誤用プロトコルに基づいて、署名M^dを算出する（ＳＴ２４ａ）。

【０１２２】続いて、署名検証装置は、第１並びに第２比較データＤ１，Ｄ２及び下記（２８）式～（３０）式のＲＳＡ共通法誤用プロトコルに基づいて、演算処理を実行し、出力Ｍを求める（ＳＴ２７ａ）。

【０１２３】

$$a1=(L^2)^{-1} \pmod{e} \quad \cdots(28)$$

$$a2=(a1L^2-1)/e \quad \cdots(29)$$

$$M=D_1^{a1}(D_2^{a2})^{-1} \pmod{N} \quad \cdots(30)$$

ここで、出力Ｍと署名対象データＳ１とが一致するとき、署名検証装置は、ユーザ装置Ｕの署名を正当と認める（ＳＴ２８ａ）。上述したように本実施形態によれば、ＲＳＡ共通法誤用プロトコルを適用可能な条件のＲＳＡ暗号系において、ｎ個の機関Ｐ１～Ｐｎに秘密鍵ｄの部分情報ｓｊが分散されたとき、ユーザ装置Ｕが、ｔ個の機関Ｔｚを選択して暗号化データＣ１を送信し、ｔ個の各機関Ｔｚが、暗号化データＣ１（＝$M^e \pmod{N}$）を演算処理して得られた部分出力Ｚｊをユーザ装置に返信し、ユーザ装置Ｕが、ｔ個の部分出力Ｚｊを合成して復号結果Ｃ２（＝$M^{L\hat{}2} \pmod{N}$）を得ると共に、復号結果Ｃ２、処理対象データＣ１及びＲＳＡ共通法誤用プロトコルに基づいて、演算処理を実行し、最終復号結果Ｍを求める。

【０１２４】これにより、分配者の無い環境で秘密鍵を算出せずに、ｎ個の機関のうち、任意ｔ個の機関による分散復号を実現することができ、また、所定条件の公開鍵を用いたラグランジュ補間法に基づき、高い確実性を実現することができる。

【０１２５】さらに、復号対象データＣ２に代えて、署名対象データＳ２（＝Ｍ）を用い、復号結果Ｃ１に代えて、署名結果Ｓ１（＝$M^{d\ L\hat{}2} \pmod{N}$、^はべき乗を示す記号）を用いることにより、ＲＳＡ共通法誤用プロトコルを用いて、演算処理を実行し、署名M^dを求める。

【０１２６】これにより、分散復号と同様に、分散署名を行うことができる。すなわち、本実施形態によれば、所定の条件で公開鍵を作成することにより、ｔ個の機関の組合せとは無関係に、確実に復号処理・署名処理を実行することができる。

【０１２７】なお、ここでノン・ディーラーモデルでの上述した機能を実現する本実施形態方式と、ディーラーモデルでの機能（（ｔ，ｎ）型での分散復号／分散署名）を実現する文献［ＦＧＭＹ９７］の方式とを比較して述べる。

【０１２８】本実施形態方式は、文献［ＦＧＭＹ９７］の方式と同じく、α，βを係数として次の（３０）式のユークリッド公式を前提とする。

【０１２９】$e\alpha+L^2\beta=1$ …（３０）

但し、gcd（ｅ，L^2）＝１

【数１３】

但し、本実施形態方式は、係数（α，β）＝〔−a2, a1〕であり、

文献［ＦＧＭＹ９７］の方式は、係数（α，β）＝（Ｐ，ｓ／Ｈ）である。

【０１３０】本実施形態方式では、復号時に部分出力Ｚｊを合成した後に、合成出力からユークリッドアルゴリズムによりＭを算出するので、このＭの算出処理の分だけ、文献［ＦＧＭＹ９７］の方式よりも処理効率が低下している（文献［ＦＧＭＹ９７］の方式は、ディーラーが鍵分散時にユークリッド公式を作成するので、復号時に各機関の部分出力を合成し、合成出力がメッセージＭとなる）。

【０１３１】しかしながら、文献［ＦＧＭＹ９７］の方式は、Ｎのオイラー関数φ（Ｎ）を知るディーラーが必要であり、$d\ P+L^2\ k \pmod{\phi(N)}$を満たす$L^2$ｋを複数の機関に秘密分散して共有する。ここで、ディーラーが秘密鍵ｄと素因数ｐ，ｑを紛失した場合、この複数の機関から秘密鍵ｄを回復できない。理由は、L^2ｋを回復しても、法φ（Ｎ）を紛失しているので、L^2ｋから秘密鍵ｄを算出できないからである。但し、法φ（Ｎ）でｄに合同な$P+L^2$ｋを算出することはできる。

【０１３２】すなわち、文献［ＦＧＭＹ９７］の方式では、ディーラーの存在する環境において、分散署名や分散復号を行えるが、ディーラーへのｄそのものの鍵回復を行えない。文献［ＦＧＭＹ９７］の方式では、鍵回復を行う際に、ディーラーモデルの文献（T. P. Pedersen, Distributed provers with applications to undeniable signatures, Advances in Cryptology-Eurocrypt 91, LNCS 547, pp.221-238, 1991.（以下、文献［Ｐｅｄ９１ａ］という））の方式又は文献［Ｏｋａ９７］の方式といった別の方式を用いる必要がある。ここで、分散ＲＳＡ暗号系における従来方式及び本発明方式の位置づけを整理すると、各方式は、図１１に示すように分類される。

【０１３３】一方、本発明方式は、ディーラーの存在する環境では、文献［Ｐｅｄ９１ａ］との組合せにより分散署名及び分散復号を実現でき、ディーラーの存在しない環境では、前述した通り、文献［ＦＭＹ９８］等との組合せにより分散署名及び分散復号を実現することができる。

【０１３４】なお、上述した第１及び第２の実施形態は、ディーラーの存在しない環境の場合を述べているので、以下に、ディーラーの存在する環境に適用する場合の変形例１，２について簡単に説明する。

【０１３５】すなわち、変形例１は、第１の実施形態をディーラーモデルに適用する場合であり、ディーラーとしてのユーザ装置Ｕは、（１３）式を満たす全ての部分秘密鍵ｄj,k を作成し、各機関に振り分ける作業を行う。この変形例１によれば、前述したステップＳＴ１～ＳＴ４までの複雑な処理を省略できる分だけ、効率を向上させることができる。

【０１３６】また、変形例２は、第２の実施形態を文献［Ｐｅｄ９１ａ］と組合せた場合であり、文献［ＦＭＹ９８］と組合せた結果と同じ機能を果たすことができる。

【０１３７】すなわち、本発明は、（ｔ，ｎ）型の秘密分散であれば、ディーラーの有無とは無関係に実現でき、上述した各実施形態に限らず、ｎ羽の鳥のうち、任意のｔ羽の鳥を異なる巣箱に入れるような関数群（K. Kurosawa and D. Stinson, Personal communication, June 1996 Referred in Desmedts paper. （Y. Desmedt,Some recent research aspects of threshold cryptography, Information Security, LNCS 1396, pp. 158-173, 1997. ））を適宜利用して実現することができる。

【０１３８】尚、本発明における記憶媒体としては、磁気ディスク、フロッピー（登録商標）ディスク、ハードディスク、光ディスク（ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ等）、光磁気ディスク（ＭＯ等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【０１３９】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【０１４０】さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【０１４１】また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【０１４２】尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【０１４３】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【０１４４】また、本発明は、ＲＳＡ暗号系に限らず、素因数分解問題に基づく暗号系であれば、ＲＳＡ暗号系以外の暗号系に適用してもよい。その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【０１４５】

【発明の効果】以上説明したように本発明によれば、分配者の無い環境で秘密鍵を算出せずに、ｎ個の機関のうち、任意ｔ個の機関による分散復号や署名を実現できる（ｔ，ｎ）型の秘密分散システム及び記憶媒体を提供できる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る秘密分散システムの構成を示す模式図

【図２】同実施形態における各機関及びユーザ装置のハードウェア構成を示すブロック図

【図３】同実施形態における秘密分散動作を説明するためのフローチャート

【図４】同実施形態における復号化動作を説明するためのフローチャート

【図５】同実施形態における署名動作を説明するためのフローチャート

【図６】同実施形態における復号可能な例を説明するための各機関の保管情報を示す模式図

【図７】同実施形態における復号不可能な例を説明するための各機関の保管情報を示す模式図

【図８】本発明の第２の実施形態における復号化動作を説明するためのフローチャート

【図９】同実施形態における署名動作を説明するためのフローチャート

【図１０】同実施形態における変形動作を説明するためのフローチャート

【図１１】従来方式と本発明方式との位置付けを示す分類図

【図１２】従来の方式における各機関に保管される部分情報の集合を示す模式図

【図１３】従来の方式における機関の組合せと対象の部分情報を示す模式図

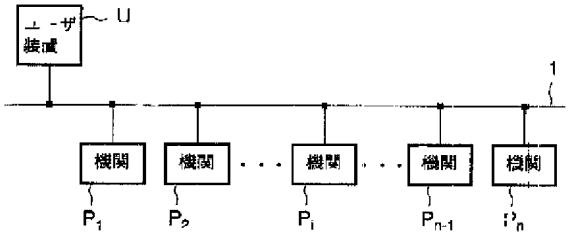
【符号の説明】

１…ネットワーク

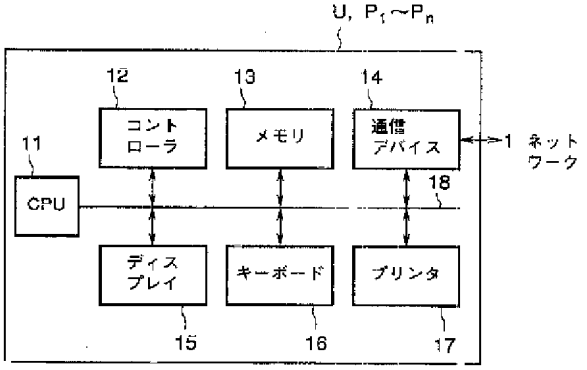
Ｕ…ユーザ装置

Ｐ１ ～Ｐｎ ，Ｐｉ …機関

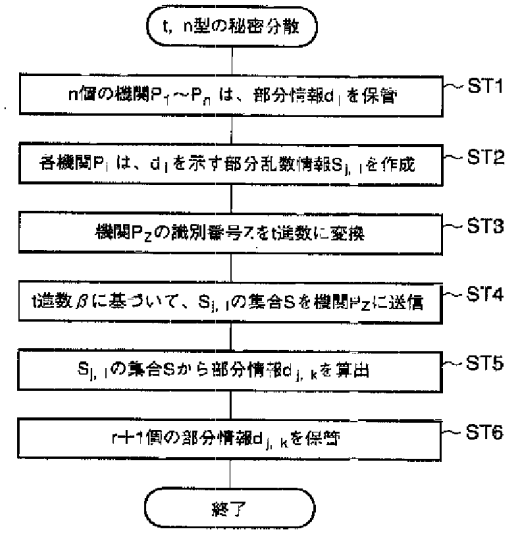
【図1】



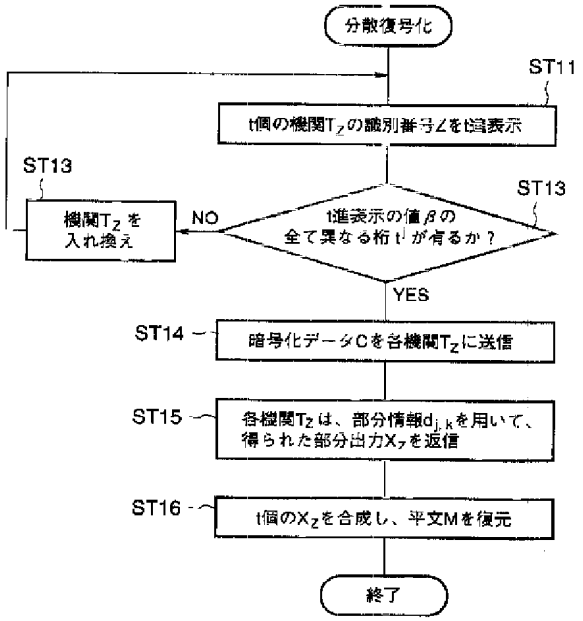
【図2】



【図3】



【図4】



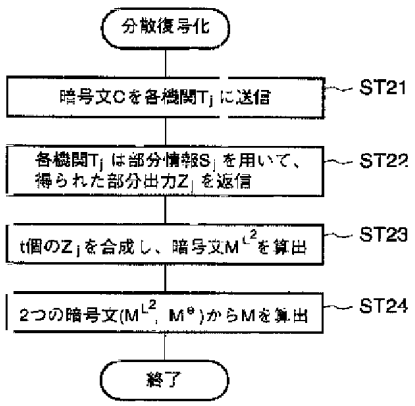
【図6】

	P20	P23	P26
3^3桁目	$d_{3,0}$	$d_{3,0}$	$d_{3,0}$
3^2桁目	$d_{2,2}$	$d_{2,2}$	$d_{2,2}$
3^1桁目	$d_{1,0}$	$d_{1,1}$	$d_{1,2}$
3^0桁目	$d_{0,2}$	$d_{0,2}$	$d_{0,2}$

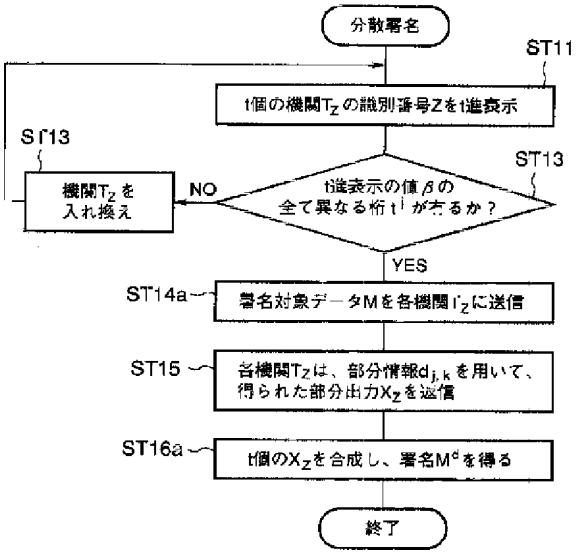
【図7】

	P20	P23	P11
3^3桁目	$d_{3,0}$	$d_{3,0}$	$d_{3,0}$
3^2桁目	$d_{2,2}$	$d_{2,2}$	$d_{2,1}$
3^1桁目	$d_{1,0}$	$d_{1,1}$	$d_{1,0}$
3^0桁目	$d_{0,2}$	$d_{0,2}$	$d_{0,2}$

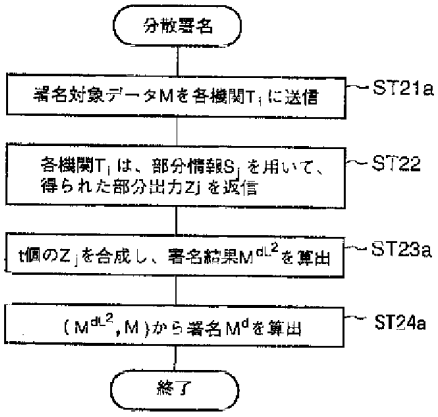
【図8】



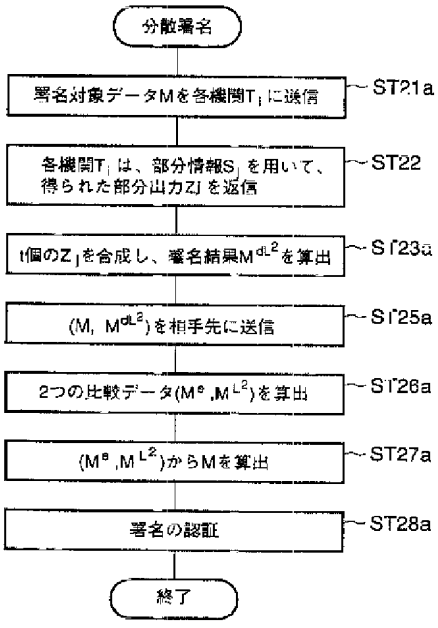
【図５】



【図９】



【図１０】



【図１１】

	ディーラーあり	ディーラーなし
[t, n] 一鍵回復	• [Ped 91a] • [Oka 97]	• [FMY 98]
[t, n] 一復号／署名	• [Ped 91a] • [FGMY 97] • [Ped 91a] 十本発明（変形例2） • ディーラーモデル+本発明（変形例1）	• [BBDW 96] • [BF 97] • [FMY 98] • [BF 97] 十本発明（第1実施形態） • [FMY 98] 十本発明（第2実施形態）

【図１２】

	X=∞	X=0	X=1	X=2
f_1	$d_{0,0}$	$d_{1,0}$	$d_{2,0}$	$d_{3,0}$
f_2	$d_{0,0}$	$d_{1,1}$	$d_{2,1}$	$d_{3,1}$
f_3	$d_{0,0}$	$d_{1,2}$	$d_{2,2}$	$d_{3,2}$
f_4	$d_{0,1}$	$d_{1,0}$	$d_{2,1}$	$d_{3,2}$
f_5	$d_{0,1}$	$d_{1,1}$	$d_{2,2}$	$d_{3,0}$
f_6	$d_{0,1}$	$d_{1,2}$	$d_{2,0}$	$d_{3,1}$
f_7	$d_{0,2}$	$d_{1,0}$	$d_{2,2}$	$d_{3,1}$
f_8	$d_{0,2}$	$d_{1,1}$	$d_{2,0}$	$d_{3,2}$
f_9	$d_{0,2}$	$d_{1,2}$	$d_{2,1}$	$d_{3,0}$

【図１３】

	X=∞		X=0		X=1		X=2
a	1, 4, 7	b	1, 2, 3	b	1, 2, 3	b	1, 2, 3
	1, 4, 8		1, 2, 6		1, 2, 5		1, 2, 4
	1, 4, 9		1, 2, 9		1, 2, 7		1, 2, 8
	1, 5, 7		1, 5, 3		1, 4, 3		1, 6, 3
	1, 5, 8		1, 5, 6		1, 4, 5		1, 6, 4
c	1, 5, 9	c	1, 5, 9	a	1, 4, 7	d	1, 6, 8
	1, 6, 7		1, 8, 3		1, 9, 3		1, 7, 3
d	1, 6, 8	d	1, 8, 6	c	1, 9, 5	a	1, 7, 4
	1, 6, 9		1, 8, 9		1, 9, 7		1, 7, 8
	2, 4, 7		4, 2, 3		6, 2, 3		5, 2, 3
	2, 4, 8		4, 2, 6		6, 2, 5		5, 2, 4
e	2, 4, 9	e	4, 2, 9	f	6, 2, 7	g	5, 2, 8
	2, 5, 7		4, 5, 3		6, 4, 3		5, 6, 3
g	2, 5, 8	h	4, 5, 6	h	6, 4, 5	h	5, 6, 4
	2, 5, 9		4, 5, 9		6, 4, 7		5, 6, 8
f	2, 6, 7	i	4, 8, 3	j	6, 9, 3	k	5, 7, 3
	2, 6, 8		4, 8, 6		6, 9, 5		5, 7, 4
	2, 6, 9		4, 8, 9		6, 9, 7		5, 7, 8
	3, 4, 7		7, 2, 3		8, 2, 3		9, 2, 3
i	3, 4, 8	f	7, 2, 6	g	8, 2, 5	e	9, 2, 4
	3, 4, 9		7, 2, 9		8, 2, 7		9, 2, 8
k	3, 5, 7	k	7, 5, 3	i	8, 4, 3	j	9, 6, 3
	3, 5, 8		7, 5, 6		8, 4, 5		9, 6, 4
	3, 5, 9		7, 5, 9		8, 4, 7		9, 6, 8
	3, 6, 7		7, 8, 3		8, 9, 3		9, 7, 3
	3, 6, 8		7, 8, 6		8, 9, 5		9, 7, 4
j	3, 6, 9	i	7, 8, 9	l	8, 9, 7	l	9, 7, 8

【手続補正書】
【提出日】平成１２年２月２日（２０００．２．２）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】００１０
【補正方法】変更
【補正内容】
【００１０】次に、総数ｎの機関における個々の機関の識別番号をｚとし（ｚ∈［０，ｎ］）、識別番号ｚの２進表示をｚ（２）＝$\beta_r\ \beta_{r-1}\ \cdots\ \beta_0$とする。ユーザは、０番目～ｎ番目の全ての機関$P_0$～$P_n$を対象とし、順次、ｚ番目の機関$P_z$に、ｒ＋１個の部分情報：$\{d_{r,\beta r}, d_{r-1,\beta r-1}, \cdots, d_{0,\beta 0}\}$を送る。これにより、全ての機関$P_0$～$P_n$には、識別番号ｚの２進表示に対応する部分情報の集合が配送される。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００２３
【補正方法】変更
【補正内容】
【００２３】但し、a_0，a_1∈F3であり、ｆ（∞）＝a_1とする。
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００６６
【補正方法】変更
【補正内容】
【００６６】
$di=S_{0,0}+S_{0,1}+\cdots+S_{0,t-2}+S_{0,t-1}$
$=S_{1,0}+S_{1,1}+\cdots+S_{1,t-2}+S_{1,t-1}$
$=\quad\cdots$
$=S_{j,0}+S_{j,1}+\cdots+S_{j,t-2}+S_{j,t-1}$
$=\quad\cdots$
$=S_{r,0}+S_{r,1}+\cdots+S_{r,t-2}+S_{r,t-1}$
次に、全ての各機関Ｐｉは、識別番号をｚとしたとき、以下のステップＳＴ３～ＳＴ４に示すように、各機関Ｐｚ（１≦ｚ≦ｎ）と互いに部分乱数情報$S_{j,1}$を分散しあう。すなわち、機関Ｐｚの識別番号ｚを（１０）式に示すように、ｔ進数に変換する（ＳＴ３）。

$$z=\beta_{r,z}t^{r}+\beta_{r-1,z}t^{r-1}+\cdots+\beta_{j,z}t^{j}+\cdots+\beta_{0,z}\quad\cdots(10)$$

簡単のため、（１０）式を（１１）式のように表記する。

$$z(t)=\beta_{r,z}\ \beta_{r-1,z}\ \cdots\ \beta_{j,z}\ \cdots\ \beta_{0,z}\quad\cdots(11)$$

但し、ｔ進値$\beta_{r,z}\in\{0,\cdots,t-1\}$

また、各機関Ｐｉは、ｚ（ｔ）における各桁ｔ^{j}毎のｔ進値βに基づいて、次に示すｒ＋１個の部分乱数情報を含む集合Ｓを機関Ｐｚに送信する（ＳＴ４）。

【手続補正４】

【補正対象書類名】明細書

【補正対象項目名】００６８

【補正方法】変更

【補正内容】

【００６８】各機関Ｐｚは、自己を含む全ての各機関Ｐ

$$z(t)=\beta_{r,z}\ \beta_{r-1,z}\ \cdots\ \beta_{0,z}$$

続いて、ユーザ装置Ｕは、ｔ個の機関Ｔａ，Ｔｂ∈Λ（ａ≠ｂ）におけるｔ進表示の各桁ｔ^{j}（０≦ｊ≦ｒ）毎に、ｔ進表示の値βが全て異なる（$\beta_{j,a}\neq\beta_{j,b}$）という条件を満たす桁ｔ^{j}が有るか否かを判定する（ＳＴ１２）。

【手続補正６】

【補正対象書類名】明細書

【補正対象項目名】００７９

【補正方法】変更

【補正内容】

【００７９】ユーザ装置は、ｔ個の各機関Ｔｚ（ｚ∈

$$f(x)=d+b1x+b2x^{2}+\cdots+b_{t-1}x^{t-1}$$

この式は、ｙ切片を秘密鍵ｄとしたｋ－１次の多項式であり、ラグランジュの補間法により、ｋ個の座標点（ｊ，ｆ(j)）から一意に定まる性質をもっている。但し、ｋ－１個の座標点からは一意に定まらず、任意のｙ切片が可能となり、秘密鍵ｄを得られない性質もある。

【手続補正８】

【補正対象書類名】明細書

【補正対象項目名】０１１３

【補正方法】変更

【補正内容】

【０１１３】すなわち、ユーザ装置Ｕは、暗号文Ｃ（＝Ｍ^{e}（ｍｏｄ Ｎ））をｔ個の各機関Ｔｊ（∈Λ）に送信する（ＳＴ２１）。各機関Ｔｊは、次の（２２）式～（２４）式の通り、それぞれ自己の部分情報ｓｊを用いて部分出力Ｚｊを算出し、得られた部分出力Ｚｊをユーザ装置Ｕに返信する（ＳＴ２２）。

$$z(t)=\beta_{r,z}\ \beta_{r-1,z}\ \cdots\ \beta_{0,z}\quad\cdots(15)$$

Λ）から受信したｔ個の部分出力Ｘｚ（ｚ∈Λ）を（１６）式のように合成し、平文Ｍを復元することができる（ＳＴ１６）。

【手続補正７】

【補正対象書類名】明細書

【補正対象項目名】０１０９

【補正方法】変更

【補正内容】

【０１０９】このとき、ｔ－１個の乱数｛b1，$\cdots b_{t-1}$｝∈Ｚに対し、（２１）式の如き、多項式を定める。

$$\cdots(21)$$

【手続補正９】

【補正対象書類名】明細書

【補正対象項目名】０１３１

【補正方法】変更

【補正内容】

【０１３１】しかしながら、文献［ＦＧＭＹ９７］の方式は、Ｎのオイラー関数ϕ（Ｎ）を知るディーラーが必要であり、ｄ≡Ｐ＋Ｌ^{2}ｋ（ｍｏｄ ϕ（Ｎ））を満たすＬ^{2}ｋを複数の機関に秘密分散して共有する。ここで、ディーラーが秘密鍵ｄと素因数ｐ，ｑを紛失した場合、この複数の機関から秘密鍵ｄを回復できない。理由は、Ｌ^{2}ｋを回復しても、法ϕ（Ｎ）を紛失しているので、Ｌ^{2}ｋから秘密鍵ｄを算出できないからである。但し、法ϕ（Ｎ）でｄに合同なＰ＋Ｌ^{2}ｋを算出することはできる。

フロントページの続き

Ｆターム(参考)　5B017 AA06 AA08 BA05 BA07 BA10
BB02 BB07 CA01 CA06 CA07
CA08 CA09 CA11 CA16
5J104 AA01 AA09 AA16 EA02 EA04
EA32 JA27 LA03 LA06 NA02